Research Paper | Computer Science | E-ISSN No : 2454-9916 | Volume : 2 | Issue : 12 | Dec 2016

3D PASSWORD: A COMPLEX AUTHENTICATION MECHANISM

Piyush Bhatia

Ramdeobaba College of Engineering and Management, Nagpur, India.

ABSTRACT

Authentication is a process of validating a user and providing security to a system. Authentication mechanisms include textual passwords, biometric passwords, site key validation etc. each having some limitations and drawbacks. To overcome these drawbacks, 3D-password came into picture as a new and improved authentication scheme. 3D-password is a multi-factor authentication scheme which includes the previous authentication schemes such as textual passwords, graphical passwords, biometric passwords etc., and adds a third dimension of a virtual environment to the previously available authentication scheme. As adding a third dimension to a picture increases its complexity, similarly adding a third dimension to the passwords makes it more complex. In this paper we explain what 3D-password is, how it is used and applied for authentication.

KEY WORDS: Authentication, Virtual environment, 3D-password.

I. INTRODUCTION

Authentication is a process of validating a user by means of a secret key (password) . The passwords can be a textual, graphical or biometric. Authentication is provided to secure data, so only an authorized user can have access to the data and use the data as it is meant to be in a non-destructive way.

Authentication can be of three types [1]:

i. The first type of authentication can be considered as having a first hand proof that the item is genuine.

ii. The second type of authentication is based on the attributes that an object possesses to prove that the object is genuine or belongs to a certain person.

iii. The third type of authentication is based on documentation. Only documents from a certain recognized authority are considered. These documents are proofs that the object is genuine.

Authentication can also be categorized based on what factors are known, that can authenticate the person before providing access to the data [1].

i. Knowledge factors: What the user knows. Example - Personal Identification Number (PIN).

ii. Ownership factors: Something possessed by the user. Example - Identification card, hardware and software tokens.

iii. Inheritance factors: What the user has inherited. Example - biometric passwords.

Another way of providing security is a two-factor authentication in which the security clearance is provided at two levels instead of one. This scheme is used for proving a higher degree of security of data which is highly confidential. Example - for doing a simple transaction at an ATM, we need our ATM card and PIN, to access the services.

Both single and two level authentication mechanisms have limitations. To overcome this, the '3D-password' scheme was introduced which provides greater security but with a higher degree of complexity. The '3D-password' scheme has a multi-factor authentication. This scheme adds a virtual environment to the authentication scheme while creating the authentication code.

II. DESCRIPTION OF THE SYSTEM

The multi-factor authentication system that the '3D-password' provides, adds the virtual environment to the already existing authentication mechanisms. The virtual environment consists of simulation of real world objects. The user interacts with those objects as done in the real world.

The virtual environment is stimulated on a personal computer or on a machine, which is capable of handling and rendering high graphics.

The choice of password scheme that the user wants depends on the user. A user can decide to use the textual or the graphical password. The password will be part of the virtual environment. The user can also decide the complexity of the password from simple to very complex.

III. SYSTEM IMPLEMENTATION

The multi-factor authentication in '3D-password' provides additional level of security for data. This extra level of security is attained using the virtual environment and the objects present in it. A user can interact with these objects in the virtual world in a way similar to that done in the real world.

The way and the sequence in which the user interacts with these objects in virtual environment create the 3D-password for the user. These interactions help the system to authenticate the user.Any input or interaction in the virtual world can become a part of the 3D-password. The objects of the virtual world can be:

i. A biometric scanner

ii. A textual password

iii. Graphical password

iv. Any real world object

v. Any future authentication scheme

Figure 1 illustrates the 3D-password authentication workflow.

Registering the 3D-password: When the user logs into the system for the first time, the virtual environment is displayed on the screen. The user then interacts with the virtual environment and the sequence of movement s/he does, is recorded. This sequence is then associated with the given user id. This user id and interaction sequence pair is then encrypted and stored in the database. This now acts as a unique and personalized username and password.

Authentication with 3D-password: The next time when the user returns, s/he enters the user id and interacts with the virtual environment. The system then fetches the sequence that is associated with the user id entered. The system compares the associated sequence with the interaction sequence, which is created during the current session. If the two sequences match, the user is authenticated and the user access is approved. Otherwise the access is declined.

The virtual environment is implemented on a machine, which has the capability of handling high graphics. Software is required to implement the virtual environment, render it, and provide the interface to the user to implement the '3D-password' scheme. The user can traverse the virtual environment with the help of an input device such as a keyboard, a mouse, a joystick, etc. Whatever interaction the user does inside the virtual environment becomes the password for the provided user id.

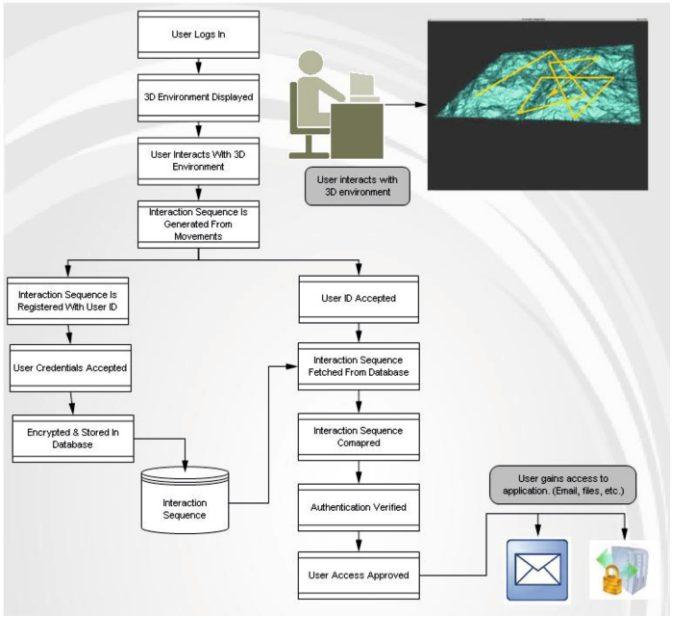

Fig. 1. Working of 3D-password

IV. PASSWORD SELECTION

The '3D-password' works in a virtual environment to provide enhanced security to the system. The entire virtual space is present onto the three axes namely, x-axis, y-axis and z-axis. Any point in the virtual space can be represented using these three axes (x, y, z). Figure 2 below shows the implementation of 3D view on a 2D screen.

Password Selection in a Virtual Environment: Imagine user in a virtual space, which is a library and the user, is traversing this virtual space using the input devices. The user first switches the lights on, the switch for which is present at a point (1, 2, 3) in the virtual space and after that goes to a computer kept on the table at the point (3, 5, 7). Then, the user turns on the monitor and enters the password to the system, which is known to the user, with the help of the keyboard present or using the virtual keyboard available, and turns off the monitor. The user then presses the go button to feed the input into the system to authenticate itself.

The sequence of user interaction, which is also the 3D-password in the virtual environment, would be

1. Switch on the lights. (1, 2, 3)
2. Turn on the monitor. (3, 5, 7)
3. Enter the password
4. Turn off the monitor

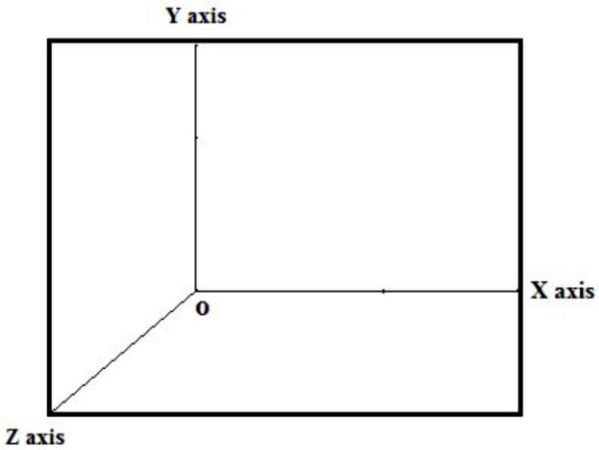

Fig. 2. 3D Virtual Environment Implementation under 2D

V. VIRTUAL ENVIRONMENT DESIGN

Virtual environment is the most important part of the 3D-password scheme as that is the medium through which the user interacts with the virtual objects. A well designed virtual environment will enhance the user experience and attract users.

3D Environment Design: Here are the guidelines [2] for designing a 3D environment:

i. **Real-life Similarities:** The virtual 3D environment should be a replica of what people are used to seeing in their day-to-day life. The virtual objects should be of a similar size as they are in real world. The response to the interaction with the virtual objects should be same as the response given in real world.

ii. **Object Uniqueness and Distinctness:** Each object present inside the virtual environment should be distinct and unique. Each object in the virtual world possesses the unique attributes of 'position'. Two similar objects in the virtual world would result in ambiguity, thereby resulting in failure of the '3D-password' scheme. The design of virtual environment should clearly distinguish between any two objects in the virtual environment. This will enhance the usability and user experience.

iii. **Size of the Virtual Environment:** The virtual environment could be as big as a city or as small as a room. The size of the virtual environment also decides the size of the 3D-password. Bigger the environment, larger the number of objects in it. As the password is sequence of user interaction with these virtual objects, a larger environment also broadens the space for password creation. With a larger password space, the time for entering the password also increases but with a smaller password space, the time required reduces.

iv. **Number of Objects and their Type:** Objects are essential to the virtual environment. Choosing the appropriate number of objects and the correct response type for these objects is very important as the objects directly affect the 3D password space.

v. **System Security:** The crux behind 3D-password scheme is the protection of the system and data. The virtual environment and the objects present should be proportional to the needed security of the system. If the information present inside the system is highly confidential then the password space should be large i.e. the size of the virtual world should be large, and the password should be complex. Larger environments can lead to higher permutation & combination of object interactions. This makes the password more secure. If the information inside the system is not that confidential then the password space should be small and the password should be simple.

VI. 3D-PASSWORD ATTRIBUTES

The 3D-password possesses the following properties [3]:

i. **Flexibility:** 3D password allows authentication through various authentication mechanisms, which are already present, and they are embedded into the 3D password scheme.

ii. **Strength:** A user's password strength depends on the number of possibilities that are possible inside the virtual environment.

iii. **Ease:** The password should be such that it can be remembered easily in the form of a short story.

iv. **Privacy:** The passwords of the users should not give out any personal information about the user. The authentication scheme should maintain the users' privacy.

VII. ATTACKS ON 3D-PASSWORD

To understand the strength of an authentication scheme, we need to understand how easy or difficult it is to break or decrypt.

In this section, we list possible attacks possible on the 3D password scheme [2].

i. **Brute Force Attack:** The attacker tires all the possible combinations that are possible to break into the system. This attack is very difficult as there are numerous possible combinations. The number of combinations depends on the number of objects present in the virtual environment. Moreover, if there are biometric scanners present in the virtual world, they will be impossible to break through.

ii. **Well-studied Attack:** The attacker tries to acquire knowledge about the password and tries the probability to crack it. In case of biometric objects, it is difficult to gather information, as forging would be required. Moreover, each 3D-password is present in a different virtual environment hence the attacker has to customize attacks according to the virtual environment present.

iii. **Shoulder Surfing:** The attacker uses a device to record what the legitimate user is doing. This is one of the most successful types of attacks possible on 3D-passwords and other graphical passwords, but this attack will be unsuccessful if the password contains certain biometric objects. For security reasons, it is advised to interact with the virtual environment in a secure place.

iv. **Timing Attacks:** In this type of attack the attacker sees how long a legitimate user takes to input the password. This gives the attacker a hint of how long the password actually is, but this is merely a hint. These attacks are suc-

cessful only if the virtual environment is poorly designed and very small with few interactions for the attacker to decode.

VIII. APPLICATIONS

The 3D-password scheme provides an authentication mechanism, which is complex than the current authentication schemes. The 3D-password has a password space, which can have numerous possible combinations that makes it difficult to crack. Moreover, it also incorporates the present day authentication mechanisms such as textual passwords, graphical passwords, biometric passwords, etc.

The 3D-password scheme is suitable to safeguard access to information or locations, which are highly confidential, and the access to these locations is highly restricted.

IX. ADVANTAGES AND DISADVANTAGES

i. Advantages:

a. 3D-Password scheme is a multi-factor authentication mechanism that incorporates all the present day authentication schemes in it.

b. Due to multiple factors involved, this scheme can generate passwords that are complex.

c. 3D-password scheme is much more secure than those currently available.

ii. Disadvantages:

a. Difficult for blind people as they cannot see the virtual environment.

b. Expensive.

c. Designing of virtual world is a challenge as it should not be very easy to crack.

d. Requires sophisticated computer designing.

X. FUTURE SCOPE

3D-password scheme uses a virtual environment for the user interaction. The rate at which the technology is growing, it will be very easy to use 3D-passwords onto handheld devices rather than only large machines.

The emergence of new technologies such as virtual reality, which has moved onto the handheld devices and also the smart wearable devices accompanied by the growth in the field of internet of things has made this authentication scheme usable for day-to-day activities like opening the door of a secured room or authenticating a user to access any other device such as laptops.

XI. CHALLENGES

The 3D-password authentication scheme works within a virtual environment that is present on a system with high processing capabilities. With the shift from traditional computing to cloud computing and distributed computing, it is difficult to add such a high rendering capacity over a network. The implementation of 3D-password for cloud computing is limited, as the network is not capable of carrying such large amount of data at a faster rate.

XII. CONCLUSION

3D-password is a multi- factor authentication scheme, which provides higher degree security to the restricted area or information. 3D-password uses virtual environment where various authentication schemes are present as a part of 3D-password. Moreover, any new upcoming authentication schemes can also be incorporated into the '3D-password' scheme. The complexity of the 3D-password depends on the size of virtual environment and the number of objects present in that environment. Designing a simple 3D-password environment leads to higher usability but compromises on the security aspect. A complex 3D-password would lead to a higher security but it won't be as easy to remember. The choice of authentication scheme will be a part of 3D-password of that user and it reflects the user's requirements.

3D-password authentication is still in early stages but, with the growth of computer graphics technology and with the incorporation of virtual reality into the handheld and wearable devices, it will not take long for 3D- password authentication scheme to be as popular as the current authentication mechanisms.

REFERENCES

[1] https://en.wikipedia.org/wiki/Authentication.

[2] A.B.Gadicha, V.B.Gadicha, —Virtual Realization using 3D Passwordl, in International Journal of Electronics and Computer Science Engineering, ISSN 2277-1956/V1N2-216-222.

[3] Duhan Pooja, Gupta Shilpi , Sangwan Sujata, & Gulati Vinita - SECURED AUTHENTICATION: 3D PASSWORD, in International Journal of Engineering and Management Sciences, ISSN 2229-600X/ VOL.3(2) 2012: 242 - 245.

[4] Fawaz A. Alsulaiman and Abdulmotaleb El Saddik, "A Novel 3D Graphical Password Schemal, IEEE International Conference on Virtual Environments, Human-Computer Interfaces, and Measurement Systems, July 2006.

[5] en.wikipedia.org/wiki/3-D_Secure.

[6] D. Weinshall and S. Kirkpatrick, "Passwords You'll Never Forget, but Can't Recall," in Proceedings of Conference on Human Factors in Computing Systems (CHI). Vienna, Austria: ACM, 2004, pp. 1399- 1402.

[7] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A.D. Rubin - "The design and analysis of graphical passwords", in Proc. 8th USENIX Security Symp, Washington DC, Aug.1999, pp.1-14.